O HACKER PROFISSIONAL

Aula de Luiz Eduardo Guarino de Vasconcelos

Objetivos

- Entender o conceito Hacker
- Oportunidades de negócios
- Exercícios para mente hacker

Hacker

- O que é um hacker para você?
- Como chegou a essa conclusão?

- Qual a visão da sociedade sobre isso?
- Qual a visão dos profissionais de TI?
- Qual a visão das empresas?
- Qual a visão da imprensa?

Hacker

- A imprensa precisa de uma palavra para denominar criminosos que usam o computador para cometer crimes, então, que palavra usar?
- **Sugestão:** Crackers, piratas de computador, cibercriminosos, hackers do mal.

Hacker

- *Hack*: Desde século XIII, vem de *to hack*, abrir caminho a golpes de machado. Hoje, abrir caminho onde os outros falharam.

  Webster, dicionário inglês

- Substantivo de dois gêneros.
  - Indivíduo hábil em descobrir falhas em sistemas de computação, podendo usar este conhecimento para o bem ou para o mal.

  Fonte: Dicionário Eletrônico Aurélio

Introdução

- **Invadir para não ser invadido é o mesmo que assaltar para não ser assaltado?**

- **Aprender como assaltar para não ser assaltado é o mesmo que aprender a invadir para não ser invadido?**
  - Vantagem: podemos invadir o próprio IP, domínios sob nossa responsabilidade e máquinas virtuais.
  - A prática do assalto sempre será crime. A da invasão não. Por que invasão (no Brasil) não é crime.

Introdução

- **Por que falar sobre hacker?**

- Pessoas ainda se surpreendem
- Atuação do hacker ainda não está clara para a sociedade.
- Imprensa, na falta de palavra melhor, relaciona o termo hacker a fraudes nos sistemas informatizados

- É "conhecimento proibido"

Introdução

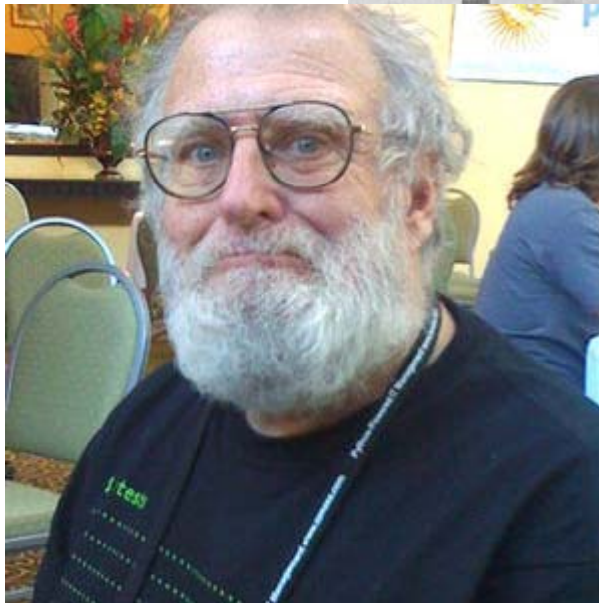
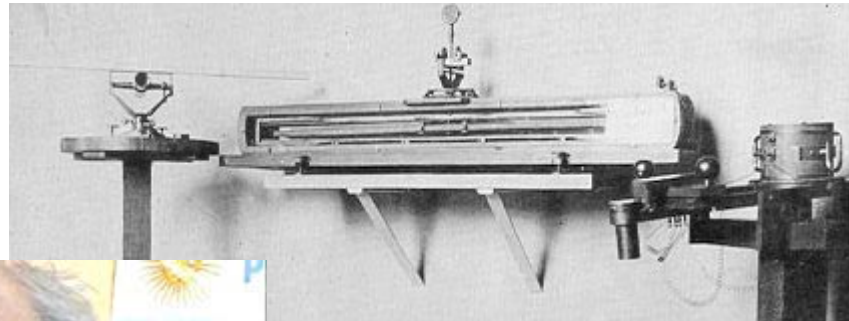
- Quem se atreve a dizer que estuda isso?
- Quem estuda o diabo?
- Quem estuda **pedofilia**?
- E a medicina com o estudo de indigentes, não é **profanação de corpos**?
- Pessoas nuas em revistas famosas é nu artístico. E se alguém quiser ser fotografado nu?
- Quem será mais bem aceito socialmente? Pedro que é fotógrafo da Playboy ou João que fotografa as vizinhas nuas?

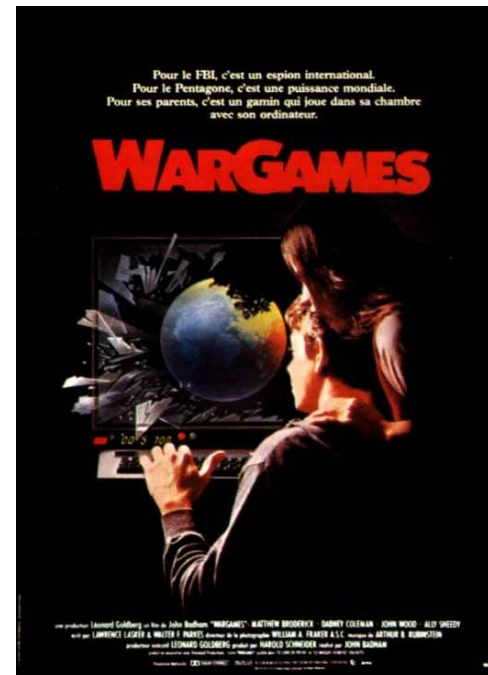
O artista e sua obra: um morto que virou escultura.

História

- Primeiros acontecimentos
  - Hacker ainda não vinculado à informática

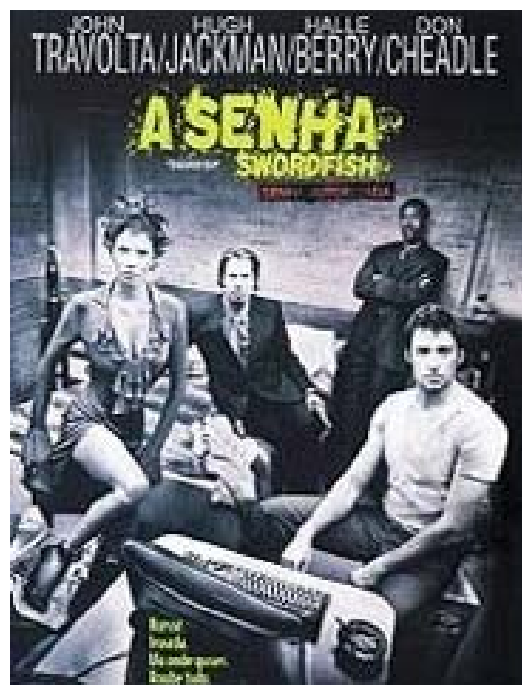
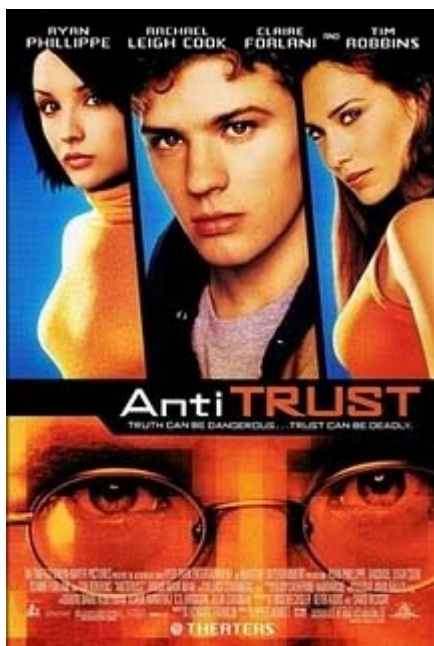
História

- Phreaking

História

- Computadores podem ser invadidos
  - Década de 70, terminais ligados à mainframes
  - Programadores colocavam trechos de código
  - Códigos que desviam centavos de contas ou salários.

História

- Script kiddies
  - Jovens começaram a ter idéias....
  - Década de 80, fase que mais teve ataque individual
  - Termo usado para crackers inexperientes.
- Caçados

História

- Precisamos deles
  - Aliança entre Indústria e Hackers
  - Conceito de Ética Hacker

Exercício 1

- Assistir Hackers Anjos ou Criminosos e entregar resenha apontando principais pontos do filme. Escrever seu ponto de vista sobre cada ponto elencado.
- Outros filmes:

- Captain ZAP – The Movie
- Hackers 2
- Os Piratas de Silicon Valley
- RevolutionOS
- The Code
- Matrix
- 007 Goldeneye
- 007 Casino Royale
- A Rede (Facebook)

O hacker profissional

- Quer ser hacker profissional?
  - Esteja ciente que é ser pioneiro
  - Sujeito a críticas e oposição
  - É o preço que se paga por sair na frente
- Profissionalizar o hacker
  - Evitar que façam parte do crime organizado ou que usem seu talento em ações de vandalismo

Ética Hacker

- Equívoco é pensar que ética hacker se relaciona com pessoa boa ou má.
- A ética hacker se refere a até que ponto o hacker é confiável.
  - Conhecer os segredos da empresa sem se aproveitar deles.
  - Imagem construída a longo prazo
- **Como confiar num hacker?**
- Se médicos e juízes são pegos cometendo crimes, que dirá hackers
- **Você concorda com a visão da ética relacionada a confiança?**

Ética Hacker

- Não existe curso de Ética, existem pessoas éticas.
- Não usar indevidamente os conhecimentos
- Compromisso moral pois não há como impedir...

Ética Hacker 1/4 (Escola de Hackers)

I. Somos contra o ganho financeiro com a obra alheia, mas a favor da livre circulação da informação.

II. Nossa função social não é corrigir falhas, mas encontrá-las.

III. Somos livres para buscar vulnerabilidades onde quer que estejam, mas nos comprometemos a divulgá-las primeiro aos responsáveis.

IV. Não denegrimos a imagem de outras pessoas e não entramos em discussões polarizadas.

V. Temos direito a liberdade de expressão, mas não ao anonimato.

Ética Hacker 2/4 (Escola de Hackers)

- VI. Temos direito ao anonimato, mas não para praticar crimes.
- VII. Sempre somos nós e o nosso avatar.
- VIII. Nos comprometemos a colaborar com as autoridades do nosso país sempre que formos requisitados.
- IX. Nos comprometemos a conhecer melhor a legislação do nosso país, ainda que seja para usá-la a nosso favor.

Ética Hacker 3/4 (Escola de Hackers)

- X. Entendemos que somos todos pessoas boas, capazes das piores maldades.
- XI. Não faremos demonstrações exibicionistas usando técnicas hacker. Nosso mérito deve vir dos hacks criados por nós, pois sem eles não temos mérito algum.
- XII. Agimos em busca de resultados. Desculpas não justificam o fracasso.
- XIII. Em nosso meio não há presunção da inocência.
- XIV. Não temos medo de nada, mas respeito por tudo.

Ética Hacker 4/4 (Escola de Hackers)

- XVI. Não somos melhores, apenas diferentes.
- XVII. Aceitamos as diferenças, mesmo quando não concordamos com elas.
- XVIII. Compartilhamos o conhecimento, nada mais.
- XIX. Defenderemos a imagem do hacker sempre que ela for deturpada pela imprensa ou por pessoa leiga.
- XX. Nunca nos intitularemos hackers. Que eles descubram quem somos.
- XXI. Nos comprometemos a buscar qualidade para nossas vidas, buscando soluções inteligentes para nossos problemas.

Como rentabilizar

- **Hacker profissional autônomo**
  - Prestação de serviço: recuperação de contas e dados, blindar o PC contra ataques.
  - Usar o buzz marketing (boca a boca). Negócio a longo prazo. Serviço não vai faltar. Impecável na forma de se apresentar e competente.
- **Caçador de vulnerabilidades (auditoria online de vulnerabilidades)**
  - Variação da anterior.
  - Para empresas que tem sites na Internet
  - Emissão de relatórios de vulnerabilidades e correções
  - Ex.: empresa Site Blindado
  - Leia http://www.siteblindado.com.br/tecnologia.html

Como rentabilizar

- **Escritor de livros hacker**
  - Experiência e habilidade
  - Web 2.0 trouxe novas vulnerabilidades. E a Web 3.0? Cloud Computing? Redes Sociais? etc
- **Instrutor de curso hacker**
  - Habilidade e experiência
  - Faltam cursos no mercado
- **Palestrante**
  - Ex.: ex-camelô David Portes
  - http://www.milpalestras.com.br/noticia.php?codigo=89 (2006)

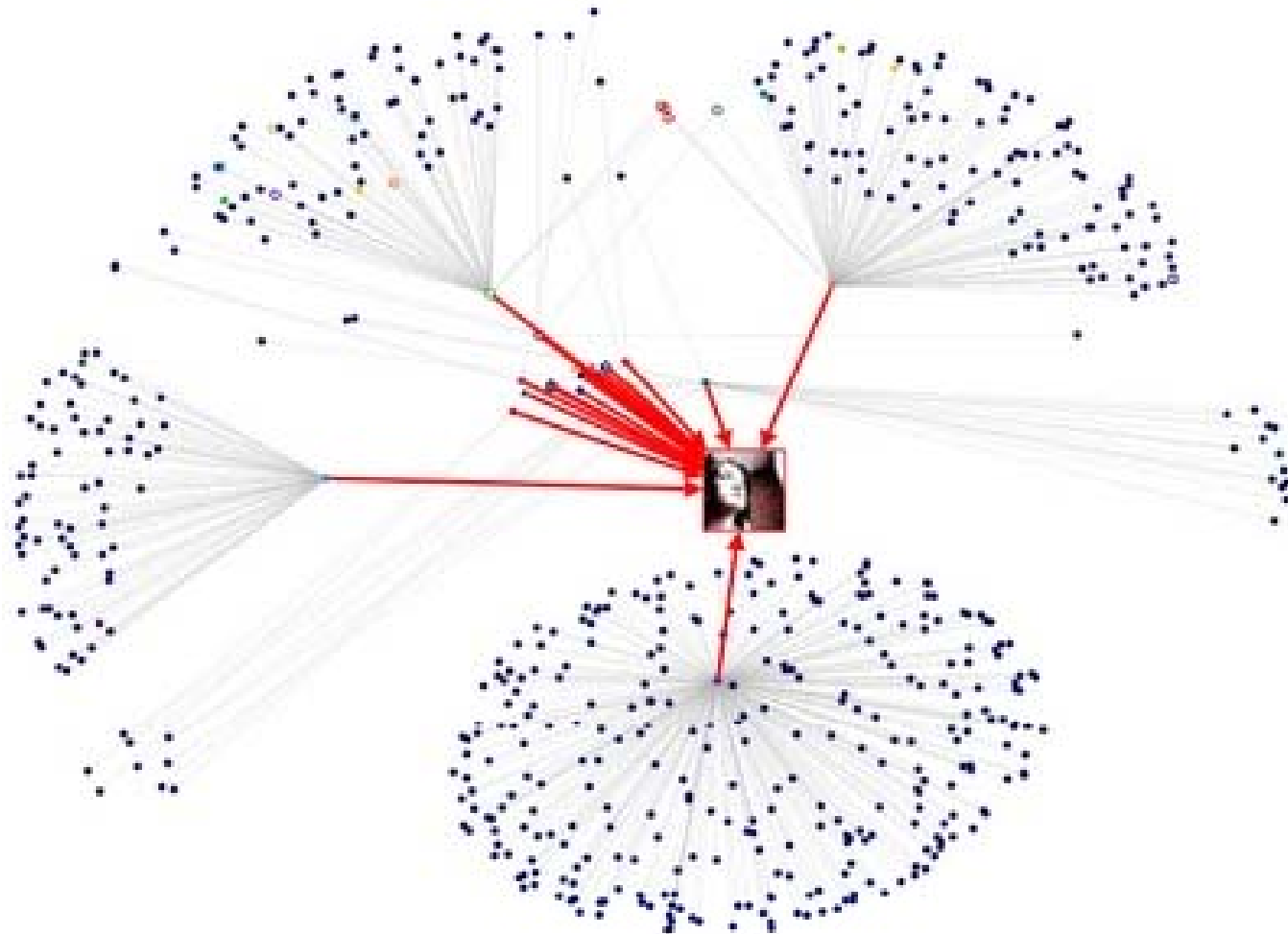
Como rentabilizar

- Quem você acha que está mais bem preparado para lidar com problemas de segurança em uma empresa? O administrador de rede, o profissional de segurança ou o hacker? Porque?

- O conhecimento de um hacker profissional é o mesmo de um profissional de segurança? Baseado em que?

Marketing pessoal

- Marketing pessoal é a criação e gerenciamento de uma imagem para o mundo, mas especificamente, para um nicho de mercado.
- Use seu **networking** para capitalizar e prestar serviços hacker.
- Prospecte novos mercados. Como fazer isto?
- O marketing pessoal começa definindo quem você quer ser (aparecer) para o mundo

Importância do Networking

Marketing pessoal
Exercício 2

- **Primeiro passo**
- Escreva a seguinte frase, substituindo QUALIDADE e ATIVIDADE pelo que é do seu interesse:

Quero ser conhecido(a) como o(a)

[UMA QUALIDADE] [UMA ATIVIDADE] [ESPAÇO GEOGRÁFICO].

- Exemplo:
  - ”Quero ser conhecido como o maior hacker do bairro.”
- Se for mais ambicioso(a):
  - ”Quero ser conhecido como o maior hacker do mundo.”

Marketing pessoal
Exercício 3

- **Segundo passo:**
- **Definindo o SER,** com a descrição do cenário.
- Um cenário é uma descrição mental de como as coisas seriam se determinada situação já existisse. Ex.: como é ser o maior hacker do mundo? O que faz o maior hacker do mundo? ...
- Responda:

- ***Como é SER?***
- ***O que FAZ?***
- ***Como as pessoas SABEM que FAZ?***
- ***O que PENSAM disso?***
- ***QUANTO ganha?***
- ***ONDE faz?***
- ***COMO faz?***
- ***Como CHEGOU lá?***

Exercício 4

- Mente hacker
  - Habilidade de buscar soluções diante de situações aparentemente sem saída
- Algumas pessoas desistem ao encontrar obstáculo, recusam-se, são incapazes.

- http://www.quizes.com.br/hacker/1.htm

- http://www.hackerskills.com/

Mente Hacker

- Desafio 4 é base para exercitar mente hacker.
- Caso não tenha reparado, avançar nas páginas do desafio teve o mesmo efeito de uma invasão, pois eram áreas protegidas que foram acessadas não por que você foi autorizado(a), mas por você ter descoberto como fazer o acesso.
- Diferentes formas de lidar. Alguns
  - Tentaram
  - Foram até onde conseguiram
  - Buscaram respostas
- Todas as formas são válidas. Tudo para alcançar o objetivo. Isto é mente hacker.

Mente hacker

- É preciso treinar
- Perder o medo
- Estudar e aceitar
- Praticar!!!

TÉCNICA, NO TECH E MENTE HACKER

Luiz Eduardo Guarino de Vasconcelos

Definição de Técnica

- Conjunto de processos, métodos e procedimentos de uma arte, ciência ou ofício (ex.: uma nova técnica para tratamento dentário).
- Jeito próprio de se fazer algo: Tenho uma técnica para memorizar.
- Prática, perícia, habilidade especial para fazer algo.

- Técnicas são chamadas **hacks**

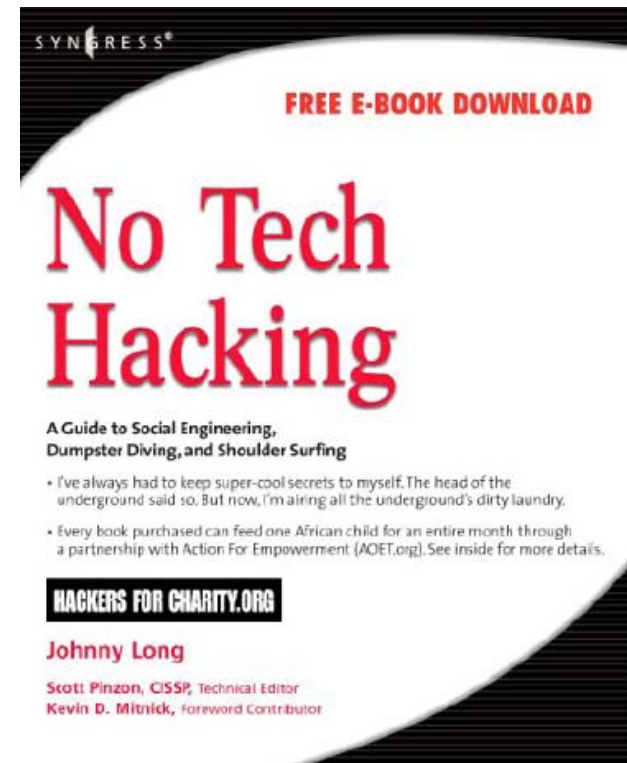
Definição de Técnica

- Aquele que cria é o mais valorizado
- Valorização não quer dizer domínio
- Às vezes, o que copia pode alcançar nível técnico maior do que aquele que cria.
- Todos usam técnicas prontas.

- Veremos algumas técnicas na disciplina
- Igual na culinária. No futuro, alguns vão copiar as receitas, outros vão adaptar e poucos vão inventar.

No Tech

- Ação Hacker sem uso de tecnologia
- Não é Sem Técnica, mas sim Sem Tecnologia

- Organizações estão se adaptando e estudando está estratégia, pois admitia-se que não seria possível atacar, contra-atacar sem tecnologia

No Tech

- Shoulder Surfing

Shoulder Surfing

Engenharia Social

No Tech

- Invasores buscam CDs e pen-drives esquecidos
- Você sabe abrir a porta do CD-ROM com o micro desligado?

Street Hacker

- Nas ruas
- Whit gadget (admite-se PDA, pen-drive com exploits, notebook, celular)
- Whitout gadget (sem uso de tecnologia)
- Busca em aeroportos, cyber café, etc

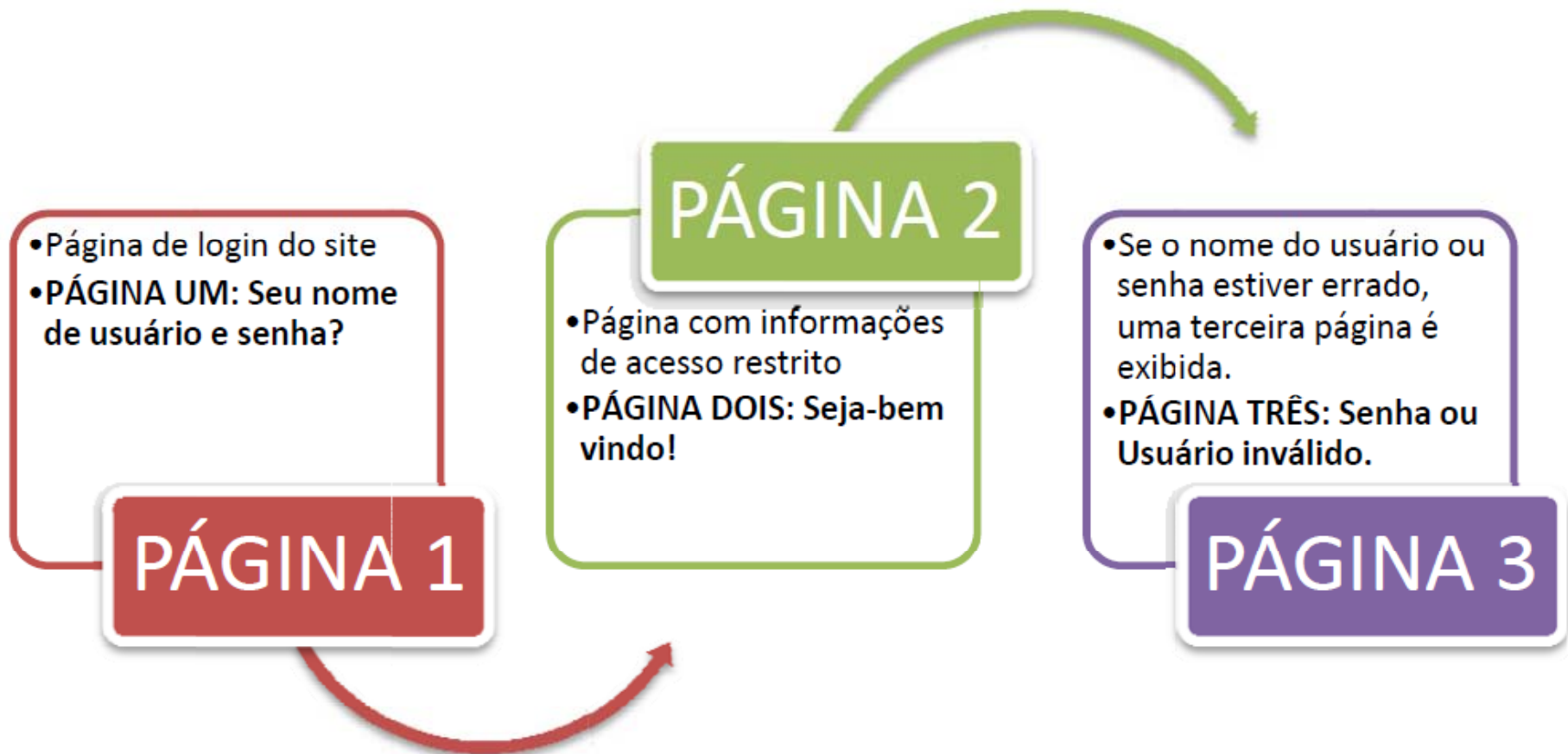
- http://www.streethacker.com/

Mente Hacker

- Toda ação é definida por um modelo mental.
- Modelo mental é a forma como seus pensamentos estão estruturados.
- Esta estruturação ocorre ao longo da vida, sendo o período de maior estruturação o que vai até os sete anos de idade. **Fase da Absorção** (informações verbais e não verbais)
- As **áreas de processamento** cerebral não usadas na infância ficam adormecidas, podendo ser despertadas a qualquer momento.
- Adultos são mais críticos e menos capazes de ir contra a estruturação já instalada e contra os **caminhos proeminentes** existentes
- Talvez estude tudo sobre hacker, mas falte reprogramar o modelo mental para começar a agir sem achar que é errado

Técnica da página dois

- **Quem você acha que cria página para Web?**
- Muitas pessoas leigas, que fez cursos de desenvolvimento de sites, de "Web Designer", etc
- **Resultado**: Páginas mal feitas ... Falta de segurança!
- **Funcionamento normal**:
  - Usuário entra na página de login e digita usuário e senha
  - O sistema verifica no banco de dados se os dados conferem, se conferir dá acesso a página dois.
  - Se os dados, nome do usuário ou senha, não conferir, o sistema exibe a página três informando o erro.

Técnica da página dois

A Vulnerabilidade

- O que acontece se o programador não proteger a página 2 do acesso direto?
  - Se você acessar a página 1 vai ter que informar usuário e senha
  - Mas e se acessar direto a página 2?
- A pergunta a responder é:
  - Qual o endereço da página 2?
  - Qual a URL permite isso?
- Isto está no código-fonte!

Demonstração

- **Demonstração**
- Acessando a página 2 de um site cobaia
- Acesso restrito autorizado sem preenchimento de usuário e senha
- Falta de validação da página 2

Exercício 6

1. Cite um No Tech diferente dos abordados em aula e descreva-o.
2. Você já obteve acesso à locais de acesso restrito? Conte-nos sua experiência.
3. Tarefa proposta:

   No decorrer dessa semana, tire a foto da tela de algum computador (que não seja o seu, obviamente).

   Faça isso em um lugar em que possa realizar o shoulder surfing sem ser percebido.

   Após tirar a foto, realize as seguintes tarefas e tire suas conclusões:

   - determine o sistema operacional utilizado;
   - determine o hardware utilizado;
   - enumere os softwares utilizados;
   - descreva demais itens, como data/hora, configurações da área de trabalho e etc.

HACKS PRONTOS PARA USO

Luiz Eduardo Guarino de Vasconcelos

Definição de Hacks

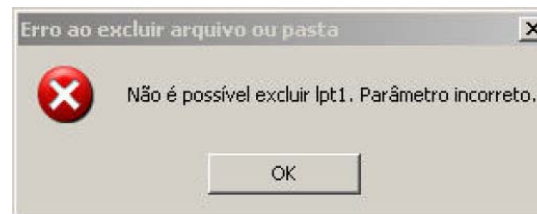
- As pessoas são o que fazem.
- Um fotógrafo é fotógrafo por fazer fotos. Um cozinheiro é cozinheiro por preparar alimentos. Um hacker é hacker por fazer hacks.
- Hacks são procedimentos que permitem obter resultados que a pessoa comum não obteria.

Hack #01 Criar pastas proibidas

- O Windows não permite a criação ou remoção de pastas com nomes de dispositivos, como por exemplo: con, lpt1, prn, com1, nul, entre outras. Experimente criar estas pastas. Se conseguir criálas, experimente removê-las.
- 1) Se você criou usando o Windows Explorer, algumas vai conseguir criar, outras não. Também terá problemas para removê-las.

Erro ao excluir arquivo ou pasta

Não é possível excluir lpt1. Parâmetro incorreto.

OK

- 2) Se você tentar criar usando a janela de prompt de comando, não vai conseguir.

Hack #2 Ver localização sem GPS

- Sites que exibem localização a partir do IP
- Não tem muita precisão e confiabilidade, mas ajuda na hora de saber de onde partiu um ataque
- http://www.myip.com.br/ **ou** http://whatismyipaddress.com/
- É hack, pois o leigo não tem a menor idéia de como fazer algo simples como verificar a provável localização de um IP e nem como fraudar esta localização.

myIP

IP:161.24.238.110

Hack #03 Encontrar MP3 no Google

- Google como ferramenta de Hacking (mais detalhes posteriormente)
  - Permite muito hacks
  - Normalmente estes links não ficam disponíveis
- Mais músicas ou cantores internacionais
- -inurl:(htm|html|php) intitle:"index of" +"last modified" +"parent directory" +description +size +(wma|mp3) "música ou cantor"
- http://www.listen77.com/free-mp3/
- http://www.gooload.com/index.html.en

Hack #04 Criar usuário no Windows sem acessar Painel de Controle

- No prompt
  - NET USER
  - NET USER hacker 123456 /ADD
- Confirme acessando **Contas de Usuário**

- Podemos gerenciar todas as contas existentes.
- Invasor pode comprometer a rede/sistema em minutos, apenas através de comandos

- Veremos mais comandos posteriormente

Exercício 7

- Como foi sua experiência com o exercício hack #1, criar pastas proibidas no Windows?
- Como foi sua experiência com o exercício hack #2, localizar sua posição pelo IP? O sistema localizou corretamente, com uma margem de erro de no máximo 50km? Conseguiu mudar a localização? Como o fez?
- Tente novamente sua localização usando o site **http://www.ip-adress.com/ipaddresstolocation**/ Notou alguma diferença? O que pode ter ocorrido?
- Como foi sua experiência com o exercício hack #3, de encontrar MP3 no Google? Qual a diferença entre buscar diretamente pelo nome da música e usar as chaves sugeridas em nossa frase de buscas?
- Como foi sua experiência com o exercício hack #4, criar o usuário no Windows? Seria possível criar um usuário na Lan House para depois acessar a rede remotamente? Como imagina que isto seja possível?

Ferramentas

- http://www.dnsgoodies.com/
  - Várias ferramentas (ping, trace, MyIP)
- http://uptime.netcraft.com/up/graph/
  - Qual sistema operacional
  - www.fatecguaratingueta.edu.br
- http://www.ussrback.com/
  - Exploits
- http://www.hostlogr.com/
  - Algumas informações do servidor

Ferramentas

- http://whois.domaintools.com/
  - Digite o domínio no formato www.nome.com e veja no final da página de resultados o IP, além de opções para refinar a busca.
  - www.fatecguaratingueta.edu.br
    - **Registro**
  - www.globo.com
    - **Mais completo**
- http://www.nomer.com.br/whois/
  - Para saber quem é o dono de um site + informações sobre o DNS.
  - www.globo.com
- http://mydnstools.info/smtprelay
  - Permite saber se um servidor permite o envio de spam:
  - smtp.globo.com

Planejamento inicial de um ataque

- Obter informações sobre o sistema
  - Monitorando a rede
  - Penetrando no sistema
  - Inserindo código ou informações falsas
  - Enviando enxurada de pacotes desnecessários, comprometendo a disponibilidade

Planejamento inicial de um ataque

- Ataques bem sucedidos podem acarretar:
  - Monitoramento não autorizado
  - Descoberta e vazamento de informações não autorizadas
  - Modificação não autorizada de servidores, base de dados e configurações
  - Negação de serviço
  - Fraude ou perdas financeiras
  - Imagem prejudicada, perda de confiança e reputação
  - Trabalho extra para a recuperação dos recursos
  - Perda de negócios, clientes e oportunidades

Planejamento inicial de um ataque

- Após ataques
  - Encobrir passos realizados
  - Exclusão de logs
  - Exclusão de arquivos criados, temporários criados
  - Formatação completa
- Importância dos IDS

Perguntas

- S ... a
  c
- S
  v

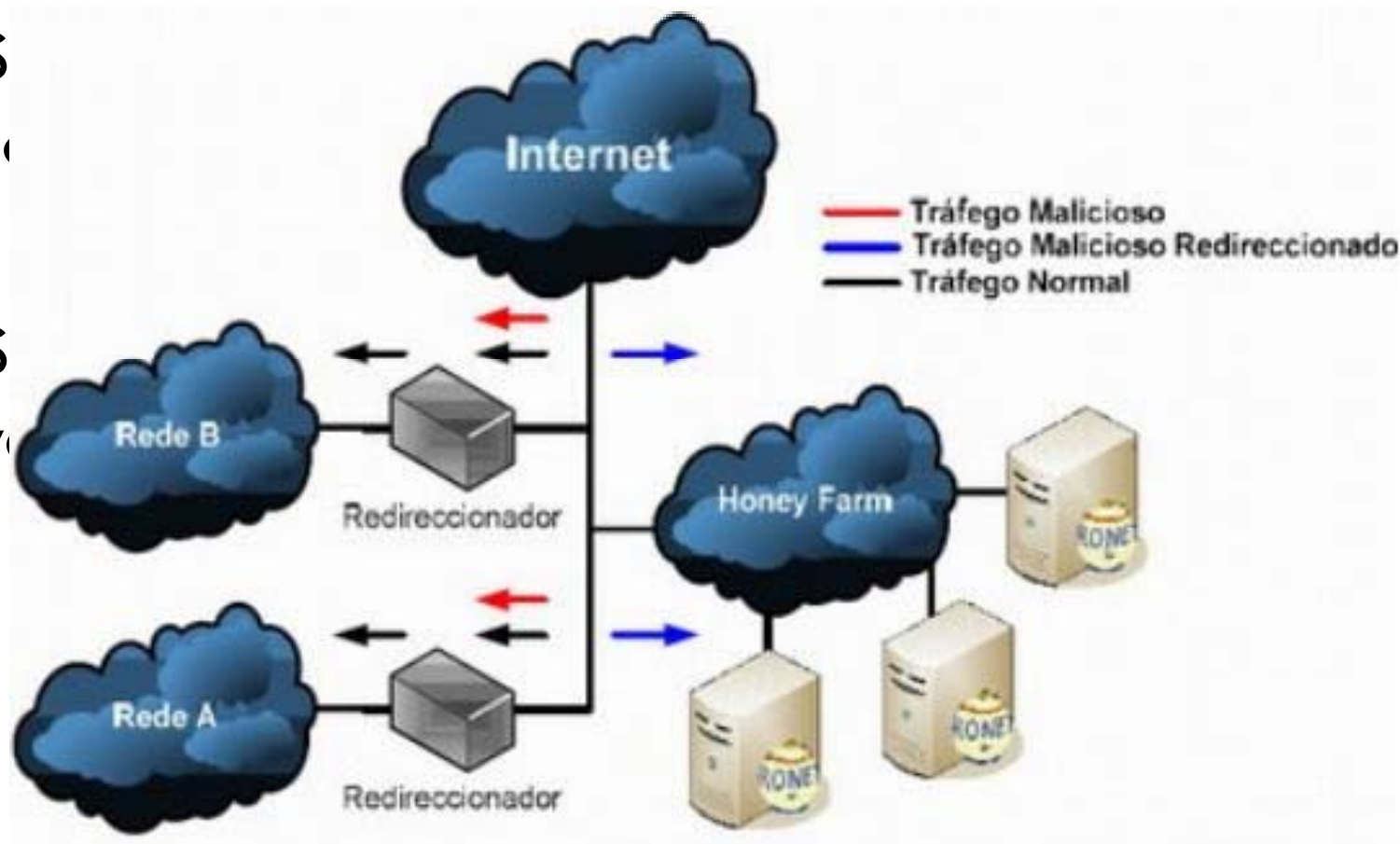



Figura 1 – Honeyfarm

Perguntas

- Se você descobre a senha de uma conta bancária é crime?
- SPAM é crime?

- O que impede você de invadir contas bancárias, desfigurar sites, acessar e-mail de terceiros, etc?
  - Medo (punição, do desconhecido, das consequências)?
  - Falta de conhecimento?
  - Algum obstáculo?

O que leva ao ataque?

- Vingança
- Vandalismo
- Terrorismo
- Patriotismo
- Religioso
- Ego
- Financeiro
- Diversão

MOTIVAÇÃO

OS RISCOS QUE RONDAM AS ORGANIZAÇÕES

Luiz Eduardo Guarino de Vasconcelos

Introdução

"O termo genérico para identificar quem realiza o ataque em um sistema computacional é hacker"

(Tissato)

Indivíduo obsessivo, de classe média, de cor branca, do sexo masculino, entre 12 e 28 anos, com pouca habilidade social e possível história de abuso físico e/ou social.

(Estudo de Marc Rogers)

Potenciais Atacantes

Segundo o Módulo Security Solutions:

- **Script kiddies:** iniciantes ou newbies
- **Cyberpunks:** mais velhos, mas ainda anti-sociais
- **Insiders**: empregados insatisfeitos
- **Coders:** os que escrevem suas 'proezas'
- **White hat**: profissionais contratados, sneakers
- **Black hat:** crackers
- **Gray hat:** hackers que vivem no limite entre white e black hat.

Usuários, autorizados ou não, também podem causar danos por erros ou ignorância.

Perdas Financeiras causados por ataques

ATAQUE	Prejuízo (U$S milhões)
Espionagem em telecomunicações	0,3
Invasão de sistema	13
Sabotagem	15,1
Negação de serviço	18,3
Abuso de rede interna	50
Roubo de laptop	11,7
Vírus	49,9
Roubo de informações proprietárias	170,8
Fraude em telecomunicações	6
Fraude financeira	115,7

Fontes de Ataque

Origem
Hackers
Funcionários internos
Concorrência
Governos estrangeiros
Empresas estrangeiras

Insiders

Funcionários confiáveis

- Venda de segredo, 1999, Área nuclear, EUA – China desde 1980

Funcionários subornados ou enganados

- Espião alemão, Karl Hinrich, seduziu funcionária, área de biotecnologia, EUA

Funcionários antigos

- 1993, José Ignacio Lopez e mais 7. GM para VW com mais de 10 mil documentos privativos de novos projetos, estratégias, etc. 1996, GM indenizada em U$S100 mi

Funcionários insatisfeitos

- Adm. Sistema insatisfeito com salário e bônus. Bomba lógica em mil computadores com prejuízo de U$S 3 mi. Março 2002.

Pontos explorados

Computador
Servidor

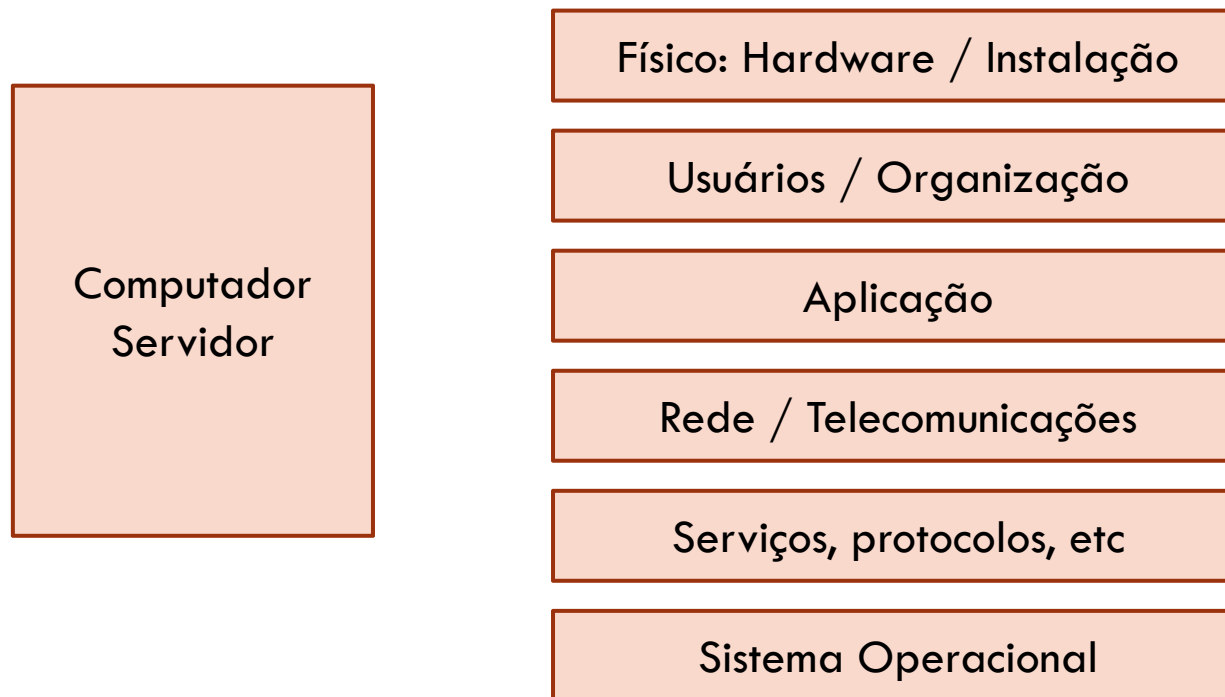
Físico: Hardware / Instalação

Usuários / Organização

Aplicação

Rede / Telecomunicações

Serviços, protocolos, etc

Sistema Operacional

Uma brecha em um desses níveis de sistemas permitirá a exploração dele todo

Ataques para a obtenção de informações

- Conhecer o terreno e coletar informações sobre o alvo sem ser notado é o primeiro passo (Tanto para atacar quanto para DEFENDER)
- **Podem ser utilizados:**
    - Dumpster diving ou trashing
    - Engenharia social
    - Ataques físicos
    - Packet sniffing
    - Port scanning
    - Scanning de vulnerabilidades
    - Firewalking
    - IP Spoofing – técnica auxiliar
    - ...

Veremos em breve

RECOMENDAÇÕES INICIAIS

Luiz Eduardo Guarino de Vasconcelos

Concepções erradas sobre segurança da informação

- “Uma vez implantada a segurança, as informações estão seguras.”
- “A implantação da segurança é um processo simples.”
- “A segurança é um assunto de exclusiva responsabilidade da área de segurança.”
- “A estrutura da segurança é relativamente estática.”

Observações

- “As portas dos fundos são tão boas quanto às portas da frente.”
- “Uma corrente é tão forte quanto o seu elo mais fraco.”
- “Um invasor não tenta transpor as barreiras encontradas, ele vai ao redor delas buscando o ponto mais vulnerável.”

As ameaças estão sempre por perto?

• Ameaça é qualquer ação ou acontecimento que possa agir sobre um ativo.
• Toda ação ou acontecimento é através de uma vulnerabilidade, gerando um determinado impacto.
• **Exemplos:**
• Naturais: raios, incêndios;
• De Negócio: fraudes, erros, sucessão de pessoas;
• Tecnológicas: mudanças, "bugs“, invasões;
• Sociais: greves, depredação, vingança;
• Culturais: impunidade;

Estamos preparados?

- Substituição de executivos
- Falha de Hardware e/ou Software
- Falha na Rede
- Invasão da Rede
- SPAM
- Falha Humana
- Espionagem

Porque se preocupar com a segurança?

- Senhas, números de cartões de crédito.
- Conta de acesso à internet.
- Dados pessoais e comerciais.
- Danificação do sistema

Porque invadir o meu computador?

- Pode ser utilizado para realizar atividades

ilícitas.(pedofilismo por exemplo).

- Realizar ataques contra outros computadores.
- Disseminar vírus.
- Enviar SPAMs.
- Furtar dados.
- Vandalismo.

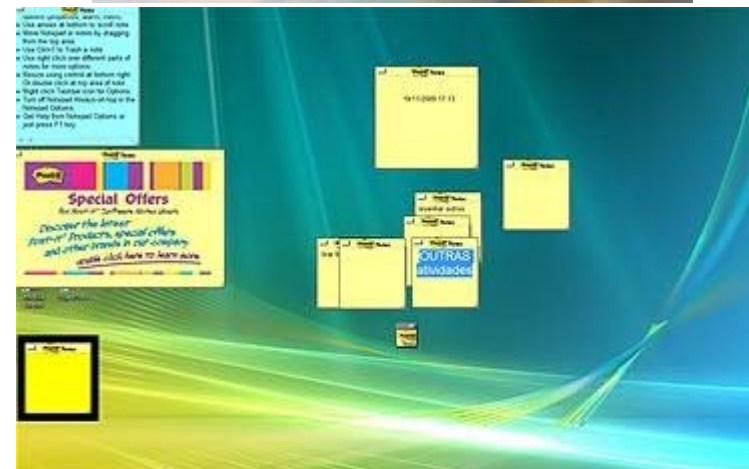
Senhas

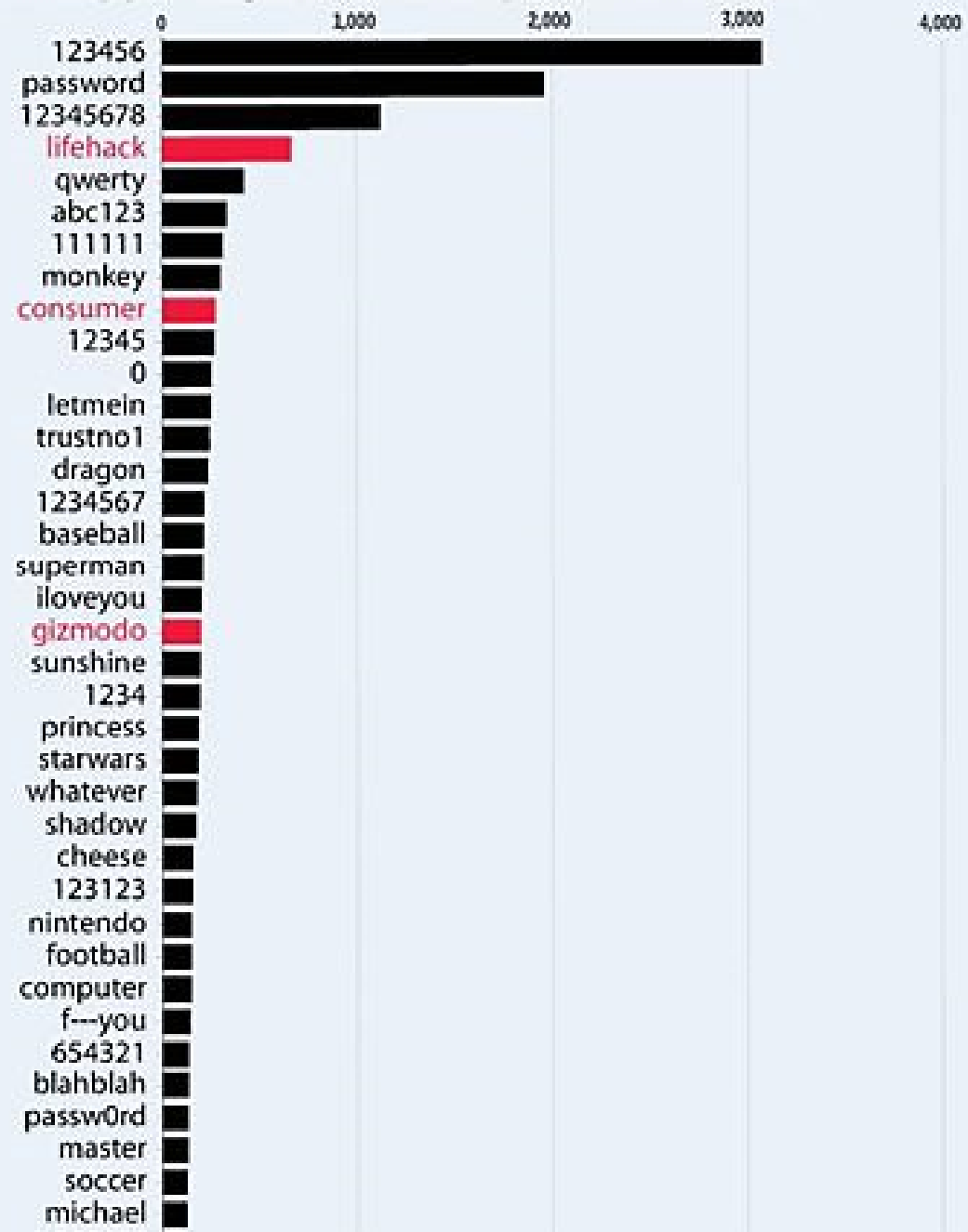
• Ler e enviar emails em seu nome.

• Obter informações pessoais suas.(Número do cartão de crédito)

• Esconder a real identidade da pessoa.

O que não usar na elaboração de senhas

- Nomes.
- Datas.
- Números de documentos.
- Números de telefone.
- Placas de carro.
- Palavras de dicionário.
- Password (Pa$$wOrd)

Como elabora

- Utilizar no mínimo 8 caracteres.
- A senha deve ser o mais “bagunçada” possível.
- Deve conter letras maiúsculas e minúsculas.
- Deve conter números.
- Deve conter caracteres especiais.
- A senha deve ser fácil de lembrar.
- “Eu sou da turma 7, de TI”
- “#E$dt7dTi”

Seja menos importante

- A preocupação com a segurança é proporcional ao que você tem a perder no caso de falha na segurança. Uma pessoa que mantém todos os seus arquivos importantes em um PC, e deixa este PC muitas horas por dia conectado por banda larga, está pondo em risco permanente a segurança das suas informações. Ser menos importante é deixar o mínimo possível à disposição dos invasores. O preço dos HDs de grande capacidade, HDs externos, pen drives a preços bastante convidativos, são boas opções para manter as informações pessoais fora do micro.

Backup Simplificado

- O backup simplificado que proponho consiste em criar pastas temáticas na estrutura do disco rígido e, se não der para fazer cópia de tudo, que copie pelo menos as pastas mais importantes. O segredo é, em vez de instalar programas de backup que você nunca vai usar, mova para as pastas os arquivos assim que são criados ou chegam ao seu PC, fazendo cópias periódicas apenas das pastas que não podem ser perdidas.

Saia do Caminho

- Quando um invasor tem acesso ao PC de alguém, a primeira coisa que faz é procurar nas pastas conhecidas por arquivos que possam conter informações importantes.
- Vai procurar em Meus documentos, raiz do disco rígido, área de trabalho, pasta das mensagens do programa de e-Mail.
- Você vai aumentar consideravelmente sua segurança se passar a armazenar seus arquivos em pastas com nomes diferentes e em locais diferentes do tradicional. Melhor, como já disse, é salvar fora do PC, usando HDs removíveis ou pen drive.

Plano de Contingência

- A visualização de cenários tanto serve para desenvolver planos de ataque como para planos de defesa. Pense na perda total do seu PC. O que aconteceria? Quais dados seriam irremediavelmente perdidos? Quanto tempo até o restabelecimento do sistema?
- Pensar na tragédia poderá sensibilizá-lo o suficiente para tomar providências imediatas em prol da segurança do seu sistema ou dos seus contratantes.
- O plano de contingência é a descrição do que você vai fazer em caso de perda total. Toda empresa deve ter um, mas a maioria nem sabe que isto existe. Cabe a você orientá-las e oferecer seus serviços.

Segurança Física

- Quando se fala em segurança da informação o leigo quase que exclusivamente se pensa em invasões e invasores. Mas segurança da informação é também segurança física.
- Prever a possibilidade de roubo, furto ou dano, seja ele natural ou por falha no equipamento.
- Inclua no seu plano de contingência previsão de segurança física também.

De quem se proteger

- As pessoas preocupam-se muito com hackers. Mas na verdade elas correm mais risco com pessoas de seu próprio convívio. A julgar pela quantidade de gente que me procura para aprender como invadir a conta de seus companheiros(as), podemos supor que o inimigo está mais próximo do que pensamos.
- Não quero pregar a desconfiança, mas alguma precaução se faz necessárias, pois o cônjuge de hoje pode ser nosso inimigo amanhã.
- O ex-prefeito de São Paulo, segundo informações que nos chegam através da imprensa, foi denunciado pela própria esposa. Recentemente tivemos o caso de um marido que, com o fim do relacionamento, divulgou um vídeo íntimo gravado com a esposa.
- A informação não está apenas no computador, mas pode parar nele.
- Cuidado com seus segredos.

Proteção

- Anti-vírus
- Firewall
- Atualização diária (e.g. Windows Update)
- Anti-spyware
- Monitorando eventos
- Monitorando processos

Proteção

- Delegacias de cibercrimes
  - http://www.safernet.org.br/site/prevencao/orientacao/delegacias
- Legislação
  - http://dsic.planalto.gov.br/documentos/quadro_legislacao.htm
- CTI (Renato Archer)
- CGI
- ISOC
- Curiosidade: Internet no Brasil
  - http://noticias.r7.com/r7/media/2010/0527_linhaTempoInternet/linhaTempoInternet_700x500.swf

Proteção

- http://www.technetbrasil.com.br
- http://www.infoguerra.com.br
- http://www.cartilha.cert.br
- http://www.modulo.com.br
- http://www.nextg.com.br
- Revistas técnicas
- Academia Latino Americana de Segurança da Informação (Microsoft)
- Internet, Internet e Internet

Exercício 9

- Usando ferramentas on-line (para 3 servidores)
  - Descobrir o endereço IP da máquina alvo.
  - Descobrir informações técnicas sobre o servidor.
  - Descobrir qual é o sistema operacional e servidor Web rodando no servidor.
  - Descrever quais ferramentas foram utilizadas

- Pode fazer até do celular
- OBS.: Considerar os IPs dos servidores

Exercício 10

- Encontre 3 “ovos de páscoa” em softwares e envie o print screen de cada um e como podem ser descobertos.
- Encontre e resuma 3 casos de espionagem ou insiders

PROFISSIONAIS

Luiz Eduardo Guarino de Vasconcelos

Profissionais

- Planejamento de carreira
- Busca de equilíbrio (profissional x pessoal)
- Valores. Ética. A ética que orienta o “caos”.

Profissionais

• Porque quanto maior a segurança, maior a facilidade de burlar a segurança?

Profissionais

- Orientado a resultados.
- Capacidade de trabalho em equipes.
- Liderança.
- Perfil empreendedor.
- Visão do futuro.
- Capacidade de inovar.
- Comunicação, expor idéias.
- Conhecimento técnico.

Profissionais

Individuais

- Orientação a resultados
- Criatividade
- Foco no cliente.
- Capacidade de análise e aprendizado.
- Trabalho em equipe.

Profissionais

- O que saber?
  - Redes e SO
  - Gestão de Projetos e TIC
  - Programação e criptologia
  - Hardware
  - Sociologia + Psicologia
- Certificações
  - Linux, Microsoft, Módulo, Cisco, ISO, CISSP

Profissionais – competências específicas

Tabela A: Resumo das Competências Específicas com base no CBK do (ISC)[2]		
Competência	**Descrição**	**Exemplos**
Arquitetura Segura	Conhecimento dos conceitos, princípios, estruturas e padrões utilizados para desenhar, programar e gerenciar um sistema computacional de forma segura.	• Desenho de uma rede de dados que possa equilibrar a manutenção dos níveis de segurança adequados e o nível de desempenho exigido pelo negócio da Organização.
Controle de Acesso	Conhecimento do conjunto de mecanismos destinados a gerenciar o modo como as pessoas podem acessar e utilizar informações.	• Aplicação do Princípio do Menor Privilégio no modo como as pessoas utilizam um Sistema Operacional, Rede de Dados ou Aplicação Corporativa.
Criptografia	Conhecimento dos princípios, meios e métodos utilizados para implementar modelos criptográficos como ferramenta de proteção para a segurança das informações de uma Organização.	• Aplicar um modelo criptográfico como camada de proteção em um sistema de pagamento que utilize a Internet como meio de transmissão de dados.

Profissionais – competências específicas

Gestão de Riscos	Conhecimento das metodologias para identificar os riscos à segurança das informações de uma Organização, dimensionamento do risco relacionado e o desenvolvimento e administração das medidas de redução de risco.	• Analisar os riscos existentes em um sistema de *e-commerce*, dimensionar o custo dos impactos da concretização de uma possível ameaça e trabalhar em conjunto com especialistas de outras áreas para desenvolver, implementar e administrar as medidas de segurança para redução dos riscos possíveis.
Legislação e Investigação	Conhecimento das leis e normas que estão relacionadas à Segurança da Informação e como devem ser utilizadas de forma agregada à Gestão da Segurança da Informação.	• Conhecer o necessário do Código Tributário Nacional para determinar o nível de disponibilidade necessário para um sistema de pagamento de impostos e desenvolver as medidas necessárias para garantir a manutenção desta disponibilidade.
Planejamento para Continuidade de Negócios e Recuperação de Desastres	Conhecimento das metodologias relacionadas ao desenvolvimento de processos que garantam a continuidade e recuperação dos negócios de uma Organização mediante uma parada inesperada.	• Entender o quão importante são os processos de negócio de uma Organização e desenvolver com base neste entendimento um modelo de contingência que permita recuperar os negócios antes que a perda torne-se inaceitavelmente custosa.

Profissionais – competências específicas

Segurança em Aplicações	Conhecimento do que é necessário fazer para criar ou administrar uma Aplicação Corporativa de modo a respeitar os conceitos de confidencialidade, integridade e disponibilidade exigidos pela Organização.	• Desenvolvimento de um modelo de segurança aplicado a todo o ciclo de desenvolvimento de uma Aplicação Corporativa (desenho, desenvolvimento, implementação e administração).
Segurança em Processos Operacionais	Conhecimento dos procedimentos que devem ser utilizados para administrar os níveis de segurança em processos operacionais que sejam utilizados no manuseio das informações.	• Conhecer e saber aplicar princípios de segurança no ciclo de vida de uma informação e distribuir procedimentos operacionais que suportem este controle em todas as áreas de uma Organização que interajam com este ciclo.

Profissionais – competências específicas

Tabela A: Resumo das Competências Específicas com base no CBK do (ISC)²		
Competência	**Descrição**	**Exemplos**
Segurança em Telecomunicações e Redes de Dados	Conhecimento dos modelos de segurança que devem ser aplicados a uma rede de dados para garantir a manutenção dos níveis de segurança esperados por uma Organização.	• Desenvolver um modelo de acesso remoto que utilize a Internet como canal de comunicação e mantenha o nível de segurança esperado, tal como uma *Virtual Private Network* (VPN).
Segurança Física e Ambiental	Conhecimento dos conceitos de segurança física e ambiental que devem ser utilizados como camada de proteção às informações de uma Organização.	• Saber desenhar os controles de segurança física adequados a um *data center* de acordo com o seu nível de criticidade para uma Organização.